UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/072,108	02/08/2002	Joseph J. Pantuso	NAI1P095/02.014.01	2543

28875 7590 02/07/2006

Zilka-Kotab, PC
P.O. BOX 721120
SAN JOSE, CA 95172-1120

EXAMINER	
PARTHASARATHY, PRAMILA	
ART UNIT	**PAPER NUMBER**
2136	

DATE MAILED: 02/07/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/072,108	PANTUSO, JOSEPH J.	
	Examiner	Art Unit	
	Pramila Parthasarathy	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *12 December 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-29* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-29* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

DETAILED ACTION

1. This action is in response to the communication filed on 12/12/2005. Claims 1 – 3, 8 – 10 and 19 – 22 are amended and Claims 23 – 29 are added. Currently Claims 1 – 29 are pending.

Double Patenting

The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., In re Berg, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); In re Goodman, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); In re Longi, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); In re Van Ornum, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); In re Vogel, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and In re Thorington, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

2. Amended Claims 1 – 29 are rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1 – 29 of U.S. Patent 6,839,852. Although the conflicting claims are not identical, they are not patentably distinct from each other because the instant case, all elements of amended Claims 1 – 29 correspond to the claims of 1 – 29 of the Patent 6,839,852 claims, except in the instant claims establishing network communications between a server computer and a plurality of client computers with firewalls over a network, wherein the firewalls are adapted for collecting information relating to intrusion activity, and include a list of trusted and banned address; collecting the information from the firewalls of the client computers utilizing the network, for identifying similar intrusion activity across a subset of the plurality of client computers; and transmitting a response to the firewalls of each of the plurality of client computers utilizing the network; wherein the firewalls are adapted for preventing the similar intrusion activity across each of the plurality of client computers utilizing the response, is referred in the Patent 6,839,852 claims as monitoring traffic events between the local computer and a remote computer over a network utilizing the firewall; logging the traffic events in an event log utilizing the firewall, wherein the event log identifies a time and an Internet Protocol (IP) address associated with the traffic events; tracing at least one of the traffic events utilizing the firewall upon the selection thereof, wherein the tracing identifies a plurality of network

segments traversed by the traffic event. It would have been obvious to one having ordinary skill in the art to recognize that collecting the information from the firewalls of the client computers utilizing the network, for identifying similar intrusion activity across a subset of the plurality of client computers; and transmitting a response to the firewalls of each of the plurality of client computers utilizing the network; wherein the firewalls are adapted for preventing the similar intrusion activity across each of the plurality of client computers utilizing the response, is equivalent to monitoring traffic events between the local computer and a remote computer over a network utilizing the firewall; logging the traffic events in an event log utilizing the firewall, tracing at least one of the traffic events utilizing the firewall upon the selection thereof, wherein the tracing identifies a plurality of network segments traversed by the traffic event.

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

3. Claims 1 – 29 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to

one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

4. The amended independent Claims 1, 8 – 10, 19 – 22 and new dependent Claims 23 and 25 recite, "subset of the plurality of client computers". The new dependent Claim 25 recites, "similar phrase sent across the subset of the plurality of client computers".

With respect to "subset of the plurality of client computers", although the specification discloses "As shown in Figure 3, network communication are initially established with a plurality of computers with firewalls over a network", see instant application page 8 lines 19 – 20, the specification does not disclose "subset of the plurality of client computers". Applicant amendment does not clarify "subset of the plurality of client computers".

The dependent claims 2 – 7, 11 – 18 and 23 – 29 are rejected at least by virtue of their dependency on the dependent claims.

With respect to "similar phrase", although the specification discloses "A plurality of the user computers (106) may be each equipped with a firewall." and "As shown in Figure 3, network communication are initially established with a plurality of computers with firewalls over a network", see instant application page 6 lines 10 – 25 and page 8 lines 19 – 20, the specification does not disclose "similar phrase". Applicant amendment does not clarify "similar phrase".

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

5. Claims 1 – 29 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

The term "similar" in claims 1 – 3, 8 – 10, 19 – 22, 24 and 25 is a relative term which renders the claim indefinite. The term "similar" is not defined by the claim, the specification does not provide a standard for ascertaining the requisite degree, and one of ordinary skill in the art would not be reasonably appraised of the scope of the invention.

The dependent claims 2 – 7, 11 – 18 and 23 – 29 are rejected at least by virtue of their dependency on the dependent claims.

Examiner will broadly interpret "similar intrusion activity" to read as "intrusion activity".

Response to Arguments

6. Applicant's arguments filed December 12, 2005 have been fully considered but they are not persuasive for the following reasons:

Applicant agrees with the Examiner that the cited prior art [Conklin et al. U.S. Patent 5,991,881, hereafter "Conklin"], discloses an Intrusion Detection portions of a Network Surveillance system". Conklin discloses a system and method for network surveillance and **detection** of attempted intrusions, or intrusions, into the network and into **computers** connected to the network. The system functions are intrusion detection **monitoring, real-time alert, logging of potential unauthorized activity, and incident progress analysis and reporting (emphasis added)**. Conklin further discloses that upon detection of any attempts to intrude, the System will initiate a log of all activity between the computer elements involved and send an alert to a monitoring console. When a log is initialed, the network continues to be monitored by a primary surveillance system. Furthermore, Conklin discloses that the system provides stand-alone network surveillance functionality, as well as **modular integration for sending alert/notification data via a data network to centralized network management systems (emphasis added)**.

Applicant argues that the Conklin does not teach, "establishing network communications between a server computer and a plurality of client computers with firewalls", "a list of trusted and banned addresses" and "identifying similar intrusion activities across a subset of the plurality of client computers". These arguments are not found persuasive. Conklin discloses, "establishing network communications between a server computer and a plurality of client computers with firewalls" (Column 3 lines 36 – 65 and Column 4 lines 9 – 28), "a list of trusted and banned addresses" (Column 4 line

45 – Column 5 line 45) and "identifying similar intrusion activities across a subset of the plurality of client computers" (Column 5 line 25 – 61).

Regarding Claim 4, Applicant argues that the Conklin does not teach, "Wherein the response includes the rules". This argument is not found persuasive. Conklin discloses, "wherein the response includes the rules" (Column 4 line 45 – Column 5 line 22 and Column 6 lines 10 – 19).

Regarding Claim 13, Applicant argues that the Conklin does not teach, "Wherein the identification of the source further includes looking up an electronic-mail address based on the IP address". This argument is not found persuasive. Conklin discloses, "wherein the identification of the source further includes looking up an electronic-mail address based on the IP address" (Column 5 line 25 – Column 6 line 12 and Column 6 line 65 – Column 7 line 23).

Regarding Claim 17, Applicant argues that the Conklin does not teach, "wherein if it is determined that the response to the notification is not received, reporting the source of the intrusion activity to a central intrusion activity watch service". This argument is not found persuasive. Conklin discloses, "wherein the identification of the source further includes looking up an electronic-mail address based on the IP address" (Column 3 lines 8 – 15 and Column 8 lines 1 – 23).

Therefore, the examiner respectfully asserts that the cited prior art does teach or suggest the amended subject matter, "establishing network communications between a server computer and a plurality of client computers with firewalls", "a list of trusted and banned addresses" and "identifying similar intrusion activities across a subset of the plurality of client computers" broadly recited in the amended independent claims 1, 8 – 10 and 19 – 22. The dependent claims 2 – 7, 11 – 18 and 23 – 29 are rejected at least by virtue of their dependency on the dependent claims and by other reason set forth in this office action. Accordingly, the rejection for the pending claims 1 – 29 is respectfully maintained.

Examiner would like to point out that although Examiner had cited particular columns and lines numbers in the references as applied to the claims for the convenience of the applicant, the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim. It is valid that other relevant passages and figures may apply as well to substitute the specified teachings. Therefore, it is respectfully requested from the applicant, in preparing the responses, to fully consider the references in entirety as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior art or disclosed by the examiner.

Claim Rejections - 35 USC § 102

The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

7. Claims 1 – 20 rejected under 35 U.S.C. 102(b) as being anticipated by Conklin et al. (U.S. Patent Number 5,991,881).

Regarding Claims 1, 8, 9, 21 Conklin teaches establishing network communications between a server computer and a plurality of client computers with firewalls over a network, wherein the firewalls are adapted for collecting information relating to intrusion activity, and include a list of trusted and banned address (Summary; Column 3 lines 37 – 43 and Column 4 line 45 – Column 5 line 45);

Collecting the information from the firewalls of the client computers utilizing the network, for identifying similar intrusion activity across a subset of the plurality of client computers (Summary; Column 3 lines 37 – 55 and Column 5 line 25 – 61); and

Transmitting a response to the firewalls of each of the plurality of client computers utilizing the network (Summary; Column 4 lines 9 – 29 and Column 5 line 25 – 61);

wherein the firewalls are adapted for preventing the similar intrusion activity across each of the plurality of client computers utilizing the response (Summary; Column 4 lines 9 – 29 and Column 5 line 25 – 61).

Regarding Claims 10, 19, 20 Conklin teaches establishing network communications between a server computer and a plurality of client computers with firewalls over a network, wherein the firewalls are adapted for collecting information relating to intrusion activity, and include a list of trusted and banned address (Summary; Column 3 lines 37 – 43 and Column 4 line 45 – Column 5 line 45);

collecting the information from the firewalls of the client computers utilizing the network (Summary; Column 3 lines 37 – 55 and Column 5 line 25 – 61);

analyzing the information to ascertain intrusion activity including similar intrusion activity across a subset of the plurality of client computers (Summary and Column 4 line 46 – Column 5 line 61);

identifying a source of the ascertained intrusion activity (Summary and Column 5 lines 9 – 29); and

notifying the source of the ascertained intrusion activity (Summary and Column 5 lines 15 – 61).

Regarding Claim 22, Conklin teaches establishing network communications between a server computer and a plurality of client computers with firewalls over a network, wherein the firewalls are adapted for collecting information relating to intrusion activity, and include a list of trusted and banned address (Summary; Column 3 lines 37 – 43 and Column 4 line 45 – Column 5 line 45);

collecting the information from the firewalls of the client computers utilizing the network, for identifying similar intrusion activity across a subset of the plurality of client computers (Summary; Column 3 lines 37 – 55 and Column 5 line 25 – 61);

heuristically analyzing the information to ascertain the similar intrusion activity (Summary and Column 4 line 46 – Column 5 line 22);

generating rules for preventing the similar intrusion activity utilizing the firewalls based on the heuristic analysis (Summary and Column 4 line 45 – Column 5 line 22);

transmitting the rules to the firewalls of the each of the plurality of client computers utilizing the network, wherein the firewalls are adapted for preventing the similar intrusion activity across each of the plurality of client computers utilizing the rules (Summary; Column 4 lines 9 – 29 and Column 5 line 25 – 61);

identifying an Internet Protocol (IP) address associated with at least one source of the similar intrusion activity (Summary and Column 5 lines 26 – 45);

looking up an electronic-mail address based on the IP address (Summary and Column 5 line 26 – Column 6 line 12);

generating a summary of the information relating to the similar intrusion activity associated with the source (Summary and Column 6 lines 20 – 27);

transmitting the summary to the electronic-mail address in the form of electronic-mail (Summary and Column 7 line 17 – Column 8 line 13);

determining whether a response to the electronic-mail is received; and if it is determined that the response to the electronic-mail is not received, reporting the source of the similar intrusion activity to a central intrusion activity watch service, wherein the

central intrusion activity watch service notifies the public of the source of the similar intrusion activity via a web interface (Summary and Column 8 lines 1 – 24).

Claim 2 is rejected as applied above in rejecting claim 1. Furthermore, Conklin teaches heuristically analyzing the information to ascertain similar intrusion activity (Summary and Column 4 line 46 – Column 5 line 22).

Claim 3 is rejected as applied above in rejecting claim 1. Furthermore, Conklin teaches generating rules for preventing the similar intrusion activity utilizing the firewalls (Summary and Column 4 line 45 – Column 5 line 22).

Claim 5 is rejected as applied above in rejecting claim 1. Furthermore, Conklin teaches wherein the information is collected by the firewalls automatically (Summary).

Claim 7 is rejected as applied above in rejecting claim 1. Furthermore, Conklin teaches wherein the information is transmitted utilizing an HTTP protocol (Summary and Column 7 lines 17 – 38).

Claim 23 is rejected as applied above in rejecting claim 1. Furthermore, Conklin teaches wherein the subset of the plurality of client computers includes a large subset of the plurality of client computers (Column 5 lines 25 – 61).

Claim 24 is rejected as applied above in rejecting claim 1. Furthermore, Conklin teaches wherein the similar intrusion activity includes a similar port scan performed across the subset of the plurality of client computers (Column 5 lines 25 – 61).

Claim 25 is rejected as applied above in rejecting claim 1. Furthermore, Conklin teaches wherein the similar intrusion activity includes an e-mail with a similar phrase sent across the subset of the plurality of client computers (Column 5 line 25 – Column 6 line 12 and Column 6 line 65 – Column 7 line 23).

Claim 26 is rejected as applied above in rejecting claim 1. Furthermore, Conklin teaches wherein a user of each of the plurality of client computers is required to subscribe in order to track the collected information and confirm the collected information (Column 1 lines 35 – 65).

Claim 27 is rejected as applied above in rejecting claim 1. Furthermore, Conklin teaches wherein the collected information is included in a report according to categories of events (Column 5 lines 1 – 44).

Claim 11 is rejected as applied above in rejecting claim 10. Furthermore, Conklin teaches wherein the information is heuristically analyzed (Summary and Column 4 line 46 – Column 5 line 22).

Claim 12 is rejected as applied above in rejecting claim 10. Furthermore, Conklin teaches wherein the identification of the source includes identifying an Internet Protocol (IP) address associated with at least one source of the intrusion activity (Summary; Column 3 lines 3 – 11 and Column 5 line 26 – Column 6 line 12).

Claim 14 is rejected as applied above in rejecting claim 10. Furthermore, Conklin teaches wherein the notification includes an electronic mail (Summary and Column 7 line 17 – Column 8 line 13).

Claim 15 is rejected as applied above in rejecting claim 10. Furthermore, Conklin teaches wherein the notification includes a summary of the intrusion activity (Summary and Column 5 lines 9 – 29).

Claim 16 is rejected as applied above in rejecting claim 10. Furthermore, Conklin teaches determining whether a response to the notification is received (Summary and Column 5 lines 9 – 29).

Claim 4 is rejected as applied above in rejecting claim 3. Furthermore, Conklin teaches wherein the response includes the rules (Summary and Column 4 line 45 – Column 5 line 22).

Claim 6 is rejected as applied above in rejecting claim 5. Furthermore, Conklin teaches wherein the information is collected by the firewalls periodically (Summary and Column 6 lines 47 – 63).

Claim 28 is rejected as applied above in rejecting claim 27. Furthermore, Conklin teaches wherein additional information associated with the collected information is reported including a time and date of when the information was collected, an Internet Protocol address associated with the collected information and applications associated with the collected information (Column 5 lines 1 – 44 and Column 8 lines 14 – 28).

Claim 29 is rejected as applied above in rejecting claim 27. Furthermore, Conklin teaches wherein the report is generated upon selection of a report icon in a graphical user interface (Column 5 lines 1 – 44 and Column 8 lines 14 – 28).

Claim 13 is rejected as applied above in rejecting claim 12. Furthermore, Conklin teaches wherein the identification of the source further includes looking up an electronic-mail address based on the IP address (Summary; Column 3 lines 3 – 11 and Column 5 line 26 – Column 6 line 12).

Claim 17 is rejected as applied above in rejecting claim 16. Furthermore, Conklin teaches wherein if it is determined that the response to the notification is not received, reporting the source of the intrusion activity to a central intrusion activity watch service (Summary and Column 8 lines 1 – 24).

Claim 18 is rejected as applied above in rejecting claim 17. Furthermore, Conklin teaches wherein the central intrusion activity watch service notifies the public of the source of the intrusion activity via a web interface (Summary and Column 7 lines 17 – 38).

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any

extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Pramila Parthasarathy whose telephone number is 571-272-3866. The examiner can normally be reached on 8:00a.m. To 5:00p.m.. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-232-3795. Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR only. For more information about the PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Pramila Parthasarathy
January 31, 2006.

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100